TESTIMONY

before the

SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION
U.S. HOUSE OF REPRESENTATIVES

by

LISA B. HIMBER
VICE PRESIDENT

MARITIME EXCHANGE FOR THE DELAWARE RIVER AND BAY

January 24, 2006

Testimony of Lisa B. Himber
January 24, 2006

Good morning, Mr. Chairman and members of the Committee, and thank you for the opportunity to present testimony today. My name is Lisa Himber, and I am Vice President of the Maritime Exchange for the Delaware River and Bay. As you may be aware, the Maritime Exchange is a non-profit trade association representing the members of the commercial maritime industry in Southern New Jersey, Southeastern Pennsylvania, and Delaware. Our mission is to promote the safety, security, economic viability and environmental health of the Delaware River port complex. Included among our 300 members are those companies and individuals on the front lines of the international border of the port – such as port authorities and private terminal operators, tug and barge companies, labor organizations, vessel operators and steamship agents, just to name a few.

In addition, I serve as Vice-Chair of the National Maritime Security Advisory Committee (NMSAC), which as you undoubtedly know was established under the Maritime Transportation Security Act (MTSA) of 2002. I and my fellow NMSAC members are charged to provide advice to the Secretary of the Department of Homeland Security on matters such as national security strategy and policy, actions required to meet current and future security threats, international cooperation on security issues, and security concerns of the maritime transportation industry.

This morning I am going to address several topics related to maritime security and federal efforts to improve it: the National Strategy for Maritime Security (NSMS), the Transportation Worker Identification Credential (TWIC), the Port Security Grant program, and the importance of expanded information sharing between the private and public sectors to enhance maritime domain awareness.

National Strategy for Maritime Security

Let me start by saying that the commercial maritime industry strongly supports the core concept behind the National Strategy for Maritime Security: to align federal security programs into a comprehensive and cohesive national effort. Since 9/11, both the Congress and the Administration have made great strides in protecting our homeland. However, in the over four years since the 9/11 attacks, there has been very little in the way of collective tangible improvements in the maritime sector. Certainly individual port facilities and businesses have implemented significant improvements in infrastructure and standard operating procedures. And the federal government has launched myriad new programs designed to mitigate threat. Yet in many respects the only visible effect of these efforts is to make it more difficult and costly to process vessels arriving at U.S. ports and the crews and cargoes they carry. It is our hope the National Strategy for Maritime Security will bring some focus to the various individual initiatives.

The Strategy has three overarching goals: to preserve the freedom of the seas, to facilitate and defend commerce, and to protect the movement of desirable goods and people. Yet

the specific objectives outlined in the plan speak only to the need to prevent attacks, protect maritime areas and infrastructures, minimize damage and expedite recovery. Many port business leaders have expressed a concern that the dual goals of threat mitigation and facilitation of trade are mutually exclusive; indeed, there are any number of instances when it can be demonstrated that compliance with new laws and regulations has led to increased direct costs of doing business as well as delays in vessel and crew processing. On the other hand, whether these efforts have prevented any security breaches is, at best, difficult to determine.

Deleted: where

In addition, it is clear that many of the federal regulations promulgated under various laws or presidential directives are simply unenforceable. The U.S. Customs and Border Protection (CBP) requirement that information concerning all persons entering the U.S. be provided to the agency in electronic format not less than 24 hours prior to arrival is an excellent example. While members of the commercial cargo industry have radically altered their business processes to accommodate this requirement, the reality is the USCBP has neither a mechanism nor the resources to enforce this regulation as it relates to the multitude of pleasure craft that enter U.S. waterways from beyond international limits. Yet the small launch operators who ferry pilots and other personnel to ships outside the port districts are required to comply. The DHS should consider implementing programs which provide a means for one-time registration of regular visitors to U.S. seaports. While a program of this nature would undoubtedly take a great deal of work to establish, we believe that in the long run it will ultimately save time and resources for both federal inspectors and the private sector.

From an industry perspective, it would be extremely helpful if indeed the National Strategy could allow us to better identify risk rather than unilaterally imposing increasing requirements and/or restrictions on all people and goods moving through our nation's seaports.

That being said, the National Maritime Security Advisory Committee was not asked by DHS to review and/or comment on the Strategy document, nor is it likely that the NSMS will be placed on the Committee agenda.

However, Committee members have dedicated their time and expertise to addressing some of the individual components of the Strategy. Currently, for example, we are in the process of developing a network of Subject Matter Experts in the various industry sub-sectors upon whom DHS can call for advice and guidance. This effort will help DHS assure continuity of the Marine Transportation System in the aftermath of an incident, which is one of the strategic actions outlined in the National Strategy for Maritime Security.

The Committee is also addressing areas of concern regarding the Memorandum of Understanding between the Coast Guard and Customs as it relates to Asymmetric Migration – or procedures to be followed to address stowaways, deserters and absconders.

However, since its inaugural meeting in March of last year, the primary effort of the NMSAC was focused on developing recommendations for implementation of the Transportation Worker Identification Credential (TWIC).

Transportation Worker Identification Credential

Having been involved in the TWIC program even prior to the establishment of the Transportation Security Administration (TSA) and the August 2002 launch of the East Coast TWIC pilot project, my organization and its members are keenly interested in the successful deployment of this program. But TWIC is not only important to the Delaware River port community; the full NMSAC membership – which includes a diverse cross-section of maritime stakeholders – unanimously concluded that TWIC is among the most important components of the national maritime security effort. As a result members elected to make TWIC the number one priority on the NMSAC agenda. Last spring, the Committee presented DHS with a full set of recommendations for TWIC implementation.

Despite the many problems with TWIC over the last several years, we continue to support the idea of a standardized credential to be used at U.S. seaports. In the first phase of the TWIC program, the planning phase, TSA did absolutely everything right. They visited with a variety of operators at differing types of ports and were thus able to understand the full range of security needs. And they talked with the people who require access to multiple facilities – including pilots and other mariners, steamship operators, trucking companies, vendors and labor – and they met with other local federal, state and municipal agencies to better understand their needs and concerns. From that effort, TSA developed what we thought would be an effective plan to move the project forward. That was in May of 2003.

As the years passed with only the slowest of progress, particularly during the third and final "prototype" phase and its overabundance of problems last year, many became disheartened. Others abandoned the effort altogether.

The TWIC program staff has worked diligently with stakeholders in an effort to sustain what remains of the pilot program, but given the ongoing delays, we are concerned about their ability to continue to do so. Today, it can only be said that at the end of the day the project has taken far longer, cost substantially more, and includes significantly less functionality than it should have done. Unfortunately, we have no confidence that TSA will be able to meet even the current deployment timetable of implementation by October of 2006.

At this point in the process, we continue to believe in the concept, but are uncertain about its viability as currently envisioned. As an immediate suggestion, we believe TSA should develop a rule that involves the full participation of industry as partners in the process. The draft of the rule has already been completed – in the form of the NMSAC recommendations. We believe it is imperative that those who work in and around our nation's ports and who understand the environment must be involved in the decisions that are made with regard to the implementation of the TWIC program.

We also believe it is important to remind DHS that the TWIC was not developed for the benefit of the federal government. The original TWIC premise – as identified by the Credentialing Direct Action Group, which started this process four years ago, and which was embraced by industry – was to standardize a credential for *those people who need access to multiple facilities*. The goal of the TWIC was to eliminate the need for truck drivers and others to pay for multiple background checks and carry multiple credentials. It would also alleviate the

need for individual port and other secure facilities to pay for the development and issuance of site-specific identification cards. These are the primary TWIC stakeholders, not the DHS.

Of particular concern now are some of the key questions surrounding the program, foremost among which is whether the federal government will manage the program or issue a standard. The MTSA, of course, requires that DHS issue this credential, and we believe that if TSA simply issues a standard, we may be back to where we were in October of 2001, with each port issuing its own cards. Other critical issues include those surrounding the background check requirements, waivers and appeals, whether an employer or sponsor would be required for a worker to obtain a TWIC, and how to include foreign seafarers and truck drivers in the program. The National Strategy for Maritime Security identifies a need for international cooperation, yet after three years of discussing the issue, the Transportation Security Administration program has not offered a solution to this last question.

NMSAC has not yet received a response from TSA to its recommendations; however we expect a briefing in the not too distant future. Our hope is that this will take place prior to publication of a proposed rulemaking, which we understand is scheduled for sometime during the first quarter of this year.

One of the reasons the Delaware River area was selected as a TWIC pilot program location was because of the work we had done prior to the events of 9/11 to develop a regional ID program for truck drivers calling multiple facilities in the tri-state region. After September 11, we quickly reprogrammed our efforts, then known as the Electronic Driver ID program, into a Delaware River ID program which would provide a standard identification to any individual requiring access to a secure facility in the region. During the first round of Port Security grants, we successfully applied for funds to expand our program. However in subsequent rounds, though the focus continues to be on projects with regional impact, the eligibility criteria have precluded regional associations from participating.

Port Security Grant Program

There are any number of opportunities for improvement which can best be made when both public and private sector port organizations work in tandem, particularly those associated with improved Maritime Domain Awareness. We have demonstrated on the Delaware River that by working together we can design programs that meet a variety of needs in both a cost-effective and timely manner. Unfortunately, though the Port Security Grant program purports to focus on enhanced regional cooperation, the grant process as it exists today does not lend itself well to regional initiatives. From the application itself, which requires the applicant to select one Congressional district, to the short time frame between announcement of eligibility criteria and application deadline – which is generally insufficient to bring interested parties together, discuss mutually agreeable project requirements, and if necessary, come to financial agreement on the required matching funds – it is difficult for communities to work together to implement regional initiatives under this program.

One example that comes to mind is the need to integrate the video surveillance images deployed by individual facilities into a common operating picture. This type of initiative would

benefit local law enforcement agencies at all levels, and regional associations can both serve as project coordinators as well as the "neutral entities" to operate such systems. The administrative processes associated with the Port Security Grant Program should be modified to allow for these types of projects and applicants.

Expanded Information Sharing to Enhance Maritime Domain Awareness

The National Security for Maritime Strategy, the Port Security Grant Program, various Presidential Directives and other communications have all highlighted the need for enhanced information sharing as critical to both incident prevention and response. As a Maritime Exchange, our group and others like us throughout the U.S. have been concerned with effective information sharing for over 130 years. While originally Exchanges were formed to share ship movement, cargo, and crew information for commercial purposes, it is obvious that DHS and other law enforcement agencies require the same information for security purposes. We strongly support federal programs which capitalize on available information to meet a variety of missions. An example is the International Trade Data System, which is being designed to streamline reporting between the private sector and multiple federal agencies. Another is the recent effort between the Coast Guard and CBP to simplify electronic crew and passenger reporting via a single program which satisfies the requirements of both agencies.

Yet there are several other opportunities to improve awareness while at the same time reducing costs for both the private and public sectors. For example, the National Strategy for Maritime Security specifically cites the development and expansion of long and short-range vessel monitoring capabilities as a key requirement to achieve Maritime Domain Awareness. The Coast Guard and industry can and should work more closely together to implement a national real-time vessel tracking system. Though Coast Guard has identified the Automated Identification System (AIS) as a priority in its Maritime Domain Awareness program and promulgated regulations that require commercial cargo vessels to carry AIS equipment on board as of December of 2004, the agency simply does not have the infrastructure to receive and monitor the AIS images across the full extent of the U.S. maritime borders. Industry has demonstrated an ability to quickly implement this technology – as well as additional long-range tracking capability that goes beyond the limited visibility AIS provides. Maritime Exchanges, Pilot Associations, and ports/harbor masters have taken the lead on these types of initiatives, and the Coast Guard can undoubtedly benefit by partnering with industry in both the funding, development and operation of vessel monitoring programs.

In addition, Exchanges, pilots and others who are entrenched in the daily business operations of their ports are uniquely qualified to assist DHS in its efforts to obtain situational awareness and to help disseminate information to users at all levels. Although we do not necessarily have access to the various targeting databases, the reality is that, unlike our federal partners, most members in the private sector have lengthy institutional memories and can quickly and easily detect anomalies in port operations. Private organizations are also well-positioned to help Captains of the Port or CBP Port Directors to add local electronic message centers, distribution lists and other functionality to existing community information systems. This would complement the work Coast Guard has undertaken on its HomePort Program, while at the same

time relieve local Coast Guard personnel from administrative tasks, thereby freeing resources for security, search and rescue, environmental protection and other critical missions.

Other examples include information sharing with regard to electronic data submitted to the federal government by ocean carriers, such as cargo manifests, advance notice of vessel arrival data, and vessel stow plan information. CBP and Coast Guard are already sharing crew/passenger information, Customs is providing cargo manifest data to port community information systems such as those operated by the Maritime Exchange, and many vessel operators are now voluntarily providing stow plan data – which they have historically shared with their port authorities and terminal operators – to CBP.

We believe there are any number of additional opportunities to share information that is useful both from security and commercial perspectives, and we look forward to continuing to work with Coast Guard and others to explore opportunities designed to meet the dual goals of improved homeland security and facilitation of commerce.

Thank you for the opportunity to speak today. I will be happy to answer any questions you may have.